



Whistler Design Preview

April 20 & 21



IPSec Security Issues for Whistler

**William Dixon,
wdixon@microsoft.com
Windows Networking &
Communications
Microsoft Corporation**

Whistler IPSec Work

Service Pack 1

- **Active Directory replication through FW protected by IPSec**
 - **Kerberos inside IPSec**
- **IETF draft update for Kerberos authentication**
 - **required to fix obscure, but potential security issue, in IETF WG last call**
- **TCPIP fix when broadcast received**
 - **avoids false “clear text received” error event message**

Whistler IPSec Work

Next Release

- **IPSec Monitor**
 - See details of IPSec state, feedback requested
- **Redesign of internal policy processing**
 - Prep for future features like API
- **Faster IPSec packet handling**
- **Deployment documentation**
 - Details on protocol & policy system implementation

Whistler IPSec Questions

- How many have tried it? In operation ?
- Where do you want to use IPSec ?
- IPSec protection from member to domain controller ?
 - Unsupported scenario in Win2k, how important ?
- IPSec Interoperability ?
- IPSec tunnel configuration UI
 - How do you want it to work ?
- IPSec policy configuration UI
 - What improvements do you need ?

Whistler IPSec Questions

- **Why is pre-shared key authentication necessary ?**
 - Provided in win2k for interop only, key string value is not securely stored
- **Additional certificate configuration ?**
 - Win2k will use any valid RSA machine certificate, not just an IPSec-only usage certificate
 - How do you want to use certificates ?

Whistler IPSec Questions

■ Need customer feedback

- Can local user or admin see active IPSec state on client ?
- Can local user or local admin see domain policy on client ?
- Can local admin change/add to domain IPSec policy on client ?
- IPSec policy API - requirements ?
 - IPSec policy configuration on platform
 - IPSec policy schema in Active

Where do you want to go today?®

Microsoft®